

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A software update device configured to communicate with a target update device via a network, the software update device comprising:

a processor configured to provide:

a certification information setting unit configured to generate a first certification information, and transmit the first certification information to the target update device over a connection via a first communication protocol over the network and request that the target update device store the first certification information, and disconnect the connection via the first communication protocol after receiving a notification that the target update device stored the first certification information;

a certification requesting unit configured to transmit the first certification information to the target update device over a connection via a second communication protocol, and request the target update device to execute a certification process with the first certification information; [[and]]

a transmitting unit configured to transmit an update software that updates a software of the target update device to the target update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol, the second communication protocol having a process load less than that of the first communication protocol; and

a certification information invalidation requesting unit configured to request the target update device to erase the first certification information subsequent to the transmittal of the update software by establishing a second connection via the second communication protocol with the target update device and determining if the target update device successfully obtained the update software, and if the update is successful, establishing

a second connection via the first communication protocol with the target update device and transmitting an erasure password to the target update device over the second connection via the first communication protocol and requesting the target update device to erase the first certification information by overwriting the first certification information with the erasure password, and disconnecting the second connection via the first communication protocol after the target update device completes overwriting the first certification information with the erasure password.

Claim 2 (Canceled).

Claim 3 (Currently Amended): The software update device as claimed in claim 1, wherein the software of the target update device is updated [[when]] after being requested by an external unit.

Claim 4 (Currently Amended): The software update device as claimed in claim 3, wherein the processor further comprising provides a notification unit configured to notify a result of updating the software of the target update device to the external unit.

Claim 5 (Previously Presented): The software update device as claimed in claim 1, wherein the first communication protocol is SSL.

Claim 6 (Previously Presented): The software update device as claimed in claim 1, wherein the second communication protocol is FTP.

Claim 7 (Previously Presented): The software update device as claimed in claim 1, wherein data transmitted via the first communication protocol is encoded, wherein data transmitted via the second communication protocol is not encoded.

Claim 8 (Currently Amended): A software update system comprising:
a software update device; and
a target update device in communication with the software update device via a network;

wherein the software update device comprises:

a processor configured to provide:

a certification information setting unit configured to generate a first certification information, and transmit the first certification information to a target update device over a connection via a first communication protocol over the network and request that the target update device store the first certification information, and disconnect the connection via the first communication protocol after receiving a notification that the target update device stored the first certification information,

a certification requesting unit configured to transmit the first certification information to the target update device over a connection via a second communication protocol, and request the target update device to execute a certification process with the first certification information, [[and]]

a transmitting unit configured to transmit an update software that updates a software of the target update device to the target update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol, the second communication protocol having a process load less than that of the first communication protocol[[;]], and

a certification information invalidation requesting unit configured to request the target update device to erase the first certification information subsequent to the transmittal of the update software by establishing a second connection via the second communication protocol with the target update device and determining if the target update device successfully obtained the update software, and if the update is successful, establishing a second connection via the first communication protocol with the target update device and transmitting an erasure password to the target update device over the second connection via the first communication protocol and requesting the target update device to erase the first certification information by overwriting the first certification information with the erasure password, and disconnecting the second connection via the first communication protocol after the target update device completes overwriting the first certification information with the erasure password;

wherein the target update device comprises:

a memory unit configured to store the first certification information, and a processor configured to provide:

a certification unit configured to execute the certification process by using the first certification information [[when]] after being requested to execute the certification process, and return a result of the certification process to the software update device, and

an updating unit configured to receive the update software [[when]] if the certification process succeeds, and update the software of the target update device.

Claim 9 (Currently Amended): The software update system as claimed in claim 8, wherein ~~the software update device further comprises a certification information invalidation~~

~~requesting unit configured to transmit an invalidation request to invalidate the first certification information to the target update device subsequent to the transmittal of the update software, and wherein the processor of the target update device is further comprises configured to provide a certification information invalidating unit configured to invalidate the first certification information [[when]] after receiving the invalidation request.~~

Claim 10 (Currently Amended): The software update system as claimed in claim 8, wherein the processor of the target update device further provides ~~comprises~~:

a restarting unit configured to restart the target update device after the software is updated by the updating unit,

a start notification transmitting unit configured to transmit a start notification informing that the target update device is started to the software update device [[when]] after the target update device is started, and

a version information transmitting unit configured to transmit version information of the target update device in response to a request from the software update device;

wherein the software update device further has a version information unit configured to obtain the version information by requesting the target update device to transmit the version information [[when]] after the start notification is received after the transmittal of the update software, and confirming the update by comparing with version information of the transmitted update software.

Claim 11 (Previously Presented): The software update system as claimed in claim 8, wherein the first communication protocol is SSL.

Claim 12 (Previously Presented): The software update system as claimed in claim 8, wherein the second communication protocol is FTP.

Claim 13 (Previously Presented): The software update system as claimed in claim 8, wherein data transmitted via the first communication protocol is encoded, wherein data transmitted via the second communication protocol is not encoded.

Claim 14 (Currently Amended): A software update method using a software update device configured to communicate with a target update device via a network, the method comprising the steps of:

generating a first certification information;
transmitting the first certification information to the target update device over a connection via a first communication protocol over the network;
requesting that the target update device store the first certification information;
disconnecting the connection via the first communication protocol after receiving a notification that the target update device stored the first certification information;
transmitting the first certification information to the target update device over a connection via a second communication protocol;
requesting the target update device to execute a certification process with the first certification information; [[and]]
transmitting an update software that updates a software of the target update device to the target update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol, the second communication protocol having a process load less than that of the first communication protocol; and

requesting the target update device to erase the first certification information
subsequent to the transmittal of the update software by establishing a second connection via
the second communication protocol with the target update device and determining if the
target update device successfully obtained the update software, and if the update is
successful, establishing a second connection via the first communication protocol with the
target update device and transmitting an erasure password to the target update device over the
second connection via the first communication protocol and requesting the target update
device to erase the first certification information by overwriting the first certification
information with the erasure password, and disconnecting the second connection via the first
communication protocol after the target update device completes overwriting the first
certification information with the erasure password.

Claim 15 (Canceled).

Claim 16 (Currently Amended): The software update method as claimed in claim 14, wherein the software of the target update device is updated [[when]] after being requested by an external unit.

Claim 17 (Original): The software update device as claimed in claim 16, further comprising a step of notifying a result of updating the software of the target update device to the external unit.

Claim 18 (Currently Amended): The software update method as claimed in claim 14, further comprising the steps of:

receiving a start notification informing that the target update device is started;

obtaining version information of the software of the target update device from the target update device [[when]] after the start notification is received after the transmittal of the update software; and

confirming the update by comparing with version information of the transmitted update software.

Claim 19 (Previously Presented): The software update method as claimed in claim 14, wherein the first communication protocol is SSL.

Claim 20 (Previously Presented): The software update method as claimed in claim 14, wherein the second communication protocol is FTP.

Claim 21 (Previously Presented): The software update method as claimed in claim 14, wherein data transmitted via the first communication protocol is encoded, wherein data transmitted via the second communication protocol is not encoded.

Claim 22 (Currently Amended): A computer readable storage medium encoded with computer executable instructions, which [[when]] if executed by a computer, cause the computer to perform a method that controls a software update device configured to communicate with a target update device via a network, the method comprising:

generating a first certification information;

transmitting the first certification information to the target update device over a connection via a first communication protocol over the network;

requesting that the target update device store the first certification information;

disconnecting the connection via the first communication protocol after receiving a notification that the target update device stored the first certification information;

transmitting the first certification information to the target update device over a connection via a second communication protocol;

requesting the target update device to execute a certification process with the first certification information; [[and]]

transmitting an update software that updates a software of the target update device to the target update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol, the second communication protocol having a process load less than that of the first communication protocol; and

requesting the target update device to erase the first certification information subsequent to the transmittal of the update software by establishing a second connection via the second communication protocol with the target update device and determining if the target update device successfully obtained the update software, and if the update is successful, establishing a second connection via the first communication protocol with the target update device and transmitting an erasure password to the target update device over the second connection via the first communication protocol and requesting the target update device to erase the first certification information by overwriting the first certification information with the erasure password, and disconnecting the second connection via the first communication protocol after the target update device completes overwriting the first certification information with the erasure password.

Claim 23 (Canceled).

Claim 24 (Currently Amended): The computer readable storage medium as claimed in claim 22, wherein the software of the target update device is updated [[when]] after being requested by an external unit.

Claim 25 (Previously Presented): The computer readable storage medium as claimed in claim 24, wherein the method further comprises notifying a result of updating the software of the target update device to the external unit.

Claim 26 (Currently Amended): The computer readable storage medium as claimed in claim 22, wherein the method further comprises:

receiving a start notification informing that the target update device is started;
obtaining version information of the software of the target update device from the target update device [[when]] after the start notification is received after the transmittal of the update software; and

confirming the update by comparing with version information of the transmitted update software.

Claim 27 (Previously Presented): The computer readable storage medium as claimed in claim 22, wherein the first communication protocol is SSL.

Claim 28 (Previously Presented): The computer readable storage medium as claimed in claim 22, wherein the second communication protocol is FTP.

Claim 29 (Previously Presented): The computer readable storage medium as claimed in claim 22, wherein data transmitted via the first communication protocol is encoded, and data transmitted via the second communication protocol is not encoded.

Claim 30 (Currently Amended): A communication device configured to communicate with a software update device via a network, the communication device comprising:

a processor configured to provide:

a certification information setting unit configured to generate certification information, and transmit the certification information to the software update device over a connection via a first communication protocol over the network, and receive a first certification information from the software update device over the connection via the first communication protocol over the network, store the first certification information, and notify the software update device that the first certification information is stored so that the software update device will close the connection via the first communication protocol;

a certifying unit configured to execute a certification process, [[when]] after receiving the first certification information from the software update device over a connection via a second communication protocol, by comparing the first certification information received over the first communication protocol with the first certification received over the second communication protocol; [[and]]

an updating unit configured to receive an update software that updates a software of the communication device from the software update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol, and update the software of the communication device,

the second communication protocol having a process load less than that of the first communication protocol; and

a certification information invalidating unit configured to invalidate the first certification information subsequent to the transmittal of the update software by establishing a second connection via the second communication protocol with the software update device and providing information to the software update device allowing the software update device to determine if the communication device successfully obtained the update software, and if the update is successful, establishing a second connection via the first communication protocol with the software update device and receiving an erasure password from the software update device over the second connection via the first communication protocol and erasing the first certification information by overwriting the first certification information with the erasure password, and disconnecting the second connection via the first communication protocol after completing overwriting the first certification information with the erasure password.

Claim 31 (Canceled).

Claim 32 (Currently Amended): The communication device as claimed in claim 30, wherein the processor further comprising provides a control [[part]] unit configured to instruct an update of the software of the communication device.

Claim 33 (Currently Amended): The communication device as claimed in claim 30, wherein the processor further provides comprising:

a restarting unit configured to restart the communication device after the software is updated;

a start notification transmitting unit configured to transmit a start notification informing that the communication device is started to the software update device [[when]] after the communication device is started, and

a version information transmitting unit configured to transmit version information of the communication device in response to a request from the software update device after the start after the transmittal of the start notification.

Claim 34 (Previously Presented): The communication device as claimed in claim 30, wherein the first communication protocol is SSL.

Claim 35 (Previously Presented): The communication device as claimed in claim 30, wherein the second communication protocol is FTP.

Claim 36 (Previously Presented): The communication device as claimed in claim 30, wherein data transmitted via the first communication protocol is encoded, wherein data transmitted via the second communication protocol is not encoded.

Claim 37 (Currently Amended): A software update system comprising:
a communication device; and
a software update device in communication with the communication device via a network;

wherein the communication device comprises:

a processor configured to provide:

a certification information setting unit configured to generate certification information, and transmit the certification information to the software

update device over a connection via a first communication protocol over the network, and receive a first certification information from the software update device over the connection via the first communication protocol, store the first certification information, and notify the software update device that the first certification information is stored so that the software update device will close the connection via the first communication protocol,

a certifying unit configured to execute a certification process, [[when]]
after receiving the first certification information from the software update device over a connection via a second communication protocol, by comparing the first certification information received over the first communication protocol with the first certification received over the second communication protocol, and

an updating unit configured to receive an update software that updates a software of the communication device from the software update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol, and update the software of the communication device, the second communication protocol having a process load less than that of the first communication protocol;

wherein the software update device comprises:

a memory unit configured to store the first certification information, and
a processor configured to provide:

a certification requesting unit configured to transmit the first certification information to the communication device, and request the communication device to execute the certification process with the first certification information, [[and]]

a transmitting unit configured to transmit the update software to the communication device via the second communication protocol over the network [[when]] if the certification process succeeds; and

a certification information invalidation requesting unit configured to request the communication device to erase the first certification information subsequent to the transmittal of the update software by establishing a second connection via the second communication protocol with the communication device and determining if the communication device successfully obtained the update software, and if the update is successful, establishing a second connection via the first communication protocol with the communication device and transmitting an erasure password to the communication device over the second connection via the first communication protocol and requesting the communication device to erase the first certification information by overwriting the first certification information with the erasure password, and disconnecting the second connection via the first communication protocol after the communication device completes overwriting the first certification information with the erasure password.

Claim 38 (Currently Amended): The software update system as claimed in claim 37, wherein the processor of the communication device further ~~comprises~~ provides a certification information invalidating unit configured to invalidate the first certification information ~~subsequent to the transmittal of the update software.~~

Claim 39 (Currently Amended): The software update system as claimed in claim 37, wherein the processor of the communication device further provides ~~comprises~~:

a restarting unit configured to restart the communication device after the software is updated,

a start notification transmitting unit configured to transmit a start notification informing that the communication device is started to the software update device [[when]] after the communication device is started, and

a version information transmitting unit configured to transmit version information of the communication device in response to a request from the software update device;

wherein the software update device further has a version information unit configured to obtain the version information by requesting the communication device to transmit the version information [[when]] after the start notification is received after the transmittal of the update software, and confirming the update by comparing with version information of the transmitted update software.

Claim 40 (Previously Presented): The software update system as claimed in claim 37, wherein the first communication protocol is SSL.

Claim 41 (Previously Presented): The software update system as claimed in claim 37, wherein the second communication protocol is FTP.

Claim 42 (Previously Presented): The software update system as claimed in claim 37, wherein data transmitted via the first communication protocol is encoded, wherein data transmitted via the second communication protocol is not encoded.

Claim 43 (Currently Amended): A software update method using a communication device configured to communicate with a software update device via a network, the method comprising the steps of:

generating certification information;

transmitting the certification information to the software update device over a first connection via a first communication protocol over the network;

receiving a first certification information from the software update device over the connection via the first communication protocol;

storing the first certification information;

notifying the software update device that the first certification information is stored so that the software update device will close the connection via the first communication protocol;

executing a certification process, [[when]] after receiving the first certification information from the software update device over a connection via a second communication protocol, by comparing the first certification information received over the first communication protocol with the first certification information received over the second communication protocol;

receiving an update software that updates a software of the communication device from the software update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol; and

updating the software of the communication device, the second communication protocol having a process load less than that of the first communication protocol; and
invalidating the first certification information subsequent to the transmittal of the update software by establishing a second connection via the second communication protocol with the software update device and providing information to the software update device

allowing the software update device to determine if the communication device successfully obtained the update software, and if the update is successful, establishing a second connection via the first communication protocol with the software update device and receiving an erasure password from the software update device over the second connection via the first communication protocol and erasing the first certification information by overwriting the first certification information with the erasure password, and disconnecting the second connection via the first communication protocol after completing overwriting the first certification information with the erasure password.

Claim 44 (Canceled).

Claim 45 (Original): The software update method as claimed in claim 43, further comprising a step of updating the software in response to an instruction to update the software from a control part.

Claim 46 (Currently Amended): The software update method as claimed in claim 43, further comprising the steps of:

restarting the communication device after the software is updated;
transmitting a start notification informing that the communication device is started to the software update device [[when]] after the communication device is started; and transmitting version information of the communication device in response to a request from the software update device after the start after the transmittal of the start notification.

Claim 47 (Previously Presented): The software update method as claimed in claim 43, wherein the first communication protocol is SSL.

Claim 48 (Previously Presented): The software update method as claimed in claim 43, wherein the second communication protocol is FTP.

Claim 49 (Previously Presented): The software update method as claimed in claim 43, wherein data transmitted via the first communication protocol is encoded, wherein data transmitted via the second communication protocol is not encoded.

Claim 50 (Currently Amended): A computer readable storage medium encoded with computer executable instructions, which [[when]] if executed by a computer, cause the computer to perform a method that controls a communication device configured to communicate with a software update device via a network, the method comprising:

- generating certification information;
- transmitting the certification information to the software update device over a first connection via a first communication protocol over the network;
- receiving a first certification information from the software update device over the connection via the first communication protocol;
- storing the first certification information;
- notifying the software update device that the first certification information is stored so that the software update device will close the connection via the first communication protocol;
- executing a certification process, [[when]] after receiving the first certification information from the software update device over a connection via a second communication protocol, by comparing the first certification information received over the first

communication protocol and the first certification information received over the second communication protocol;

receiving an update software that updates a software of the communication device from the software update device via the second communication protocol over the network [[when]] if the certification process succeeds via the second communication protocol; [[and]]

updating the software of the communication device, the second communication protocol having a process load less than that of the first communication protocol; and

invalidating the first certification information subsequent to the transmittal of the update software by establishing a second connection via the second communication protocol with the software update device and providing information to the software update device allowing the software update device to determine if the communication device successfully obtained the update software, and if the update is successful, establishing a second connection via the first communication protocol with the software update device and receiving an erasure password from the software update device over the second connection via the first communication protocol and erasing the first certification information by overwriting the first certification information with the erasure password, and disconnecting the second connection via the first communication protocol after completing overwriting the first certification information with the erasure password.

Claim 51 (Canceled).

Claim 52 (Previously Presented): The computer readable storage medium as claimed in claim 50, wherein the method further comprises updating the software in response to an instruction to update the software from a control part.

Claim 53 (Currently Amended): The computer readable storage medium as claimed in claim 50, wherein the method further comprises:

restarting the communication device after the software is updated;
transmitting a start notification informing that the communication device is started to the software update device [[when]] after the communication device is started; and
transmitting version information of the communication device in response to a request from the software update device after the start after the transmittal of the start notification.

Claim 54 (Previously Presented): The computer readable storage medium as claimed in claim 50, wherein the first communication is SSL.

Claim 55 (Previously Presented): The computer readable storage medium as claimed in claim 50, wherein the second communication protocol is FTP.

Claim 56 (Previously Presented): The computer readable storage medium as claimed in claim 50, wherein data transmitted via the first communication protocol is encoded, and data transmitted via the second communication protocol is not encoded.